

A chaos-based approach for information hiding security

Jacques M. Bahi, Senior Member IEEE
Christophe Guyeux

Computer Science Laboratory LIFC
University of Franche-Comte, France

Abstract. This paper introduces a new framework for data hiding security. Contrary to the existing ones, the approach introduced here is not based on probability theory. In this paper, a scheme is considered as secure if its behavior is proven unpredictable. The objective of this study is to enrich the existing notions of data hiding security with a new rigorous and practicable one. This new definition of security is based on the notion of topological chaos. It could be used to reinforce the confidence on a scheme previously proven as secure by other approaches and it could also be used to study some classes of attacks that currently cannot be studied by the existing security approaches. After presenting the theoretical framework of the study, a concrete example is detailed in order to show how our approach can be applied.

Keywords: Information hiding security, Theory of chaos, Spread-spectrum.

1 Introduction

In past decades, the studies in the information hiding domain have almost exclusively been focused on robustness [1], [8]. Security has emerged in the last years as a new interest in this domain [9], [24], [26]. Security and robustness are neighboring concepts without clearly established definitions [25]. Robustness is often considered to be mostly concerned by blind elementary attacks, whereas security is not limited to certain specific attacks. Security encompasses robustness and intentional attacks [13], [20]. The attempts to define the differences between robustness and security, to clarify the classes of attacks and to give some consistency to the notion of security, illustrates the recent important concern to bring a rigorous theoretical framework for security in data hiding.

In the framework of watermarking and steganography, security has seen several important developments since the last decade. Nevertheless, several open questions still remain. For example, the current theoretical approach requires strong hypotheses on the covertext and these hypotheses are quite difficult to evaluate in practice. Moreover, even if several security classes have been identified since the first classification of attacks, only a small part of them can be easily studied within this framework. In the existing approach, when a same

hidden message is embedded into several covertexts, information leak is studied in terms of probability. If the leak is important, then the scheme is considered as insecure. In this paper we are interested in the evaluation of unpredictability of a data hiding scheme: this last is considered as secure if it is proven to be unpredictable. This new framework can be used to study some classes of attacks that are difficult to investigate in the existing security approach. It also enriches the variety of qualitative and quantitative tools that evaluate how strong the security is, thus reinforcing the confidence that can be put on a given scheme. Indeed, let us suppose that Eve, an attacker, observes the behavior of a data hiding machine. If there is no information leak, when Eve applies an input on the machine, and if nothing can be understood when the input is changing, because of the unpredictable behavior of the machine, so she cannot deduce much things from these observations. This claim is discussed more rigorously in Section 4.

The rest of this paper is organized as follows. In Section 2, related work concerning data hiding security is recalled. Our contribution in relation to existing framework is explained. In Section 3, the definition of chaos used in this paper is presented, the notion of chaotic-security is defined and the feasibility of its study in real-world applications is established. An illustrative example is given in Section 4: the chaotic-security study of various spread-spectrum data hiding schemes is presented and the level of security is qualitatively and quantitatively evaluated. The link between chaotic-security and stego-security is discussed and the impact of our study in regard to various classes of attacks is detailed. The paper ends with a conclusion where our contribution is summarized, and planned future work is discussed.

2 Related work and contribution

2.1 Related work

The first fundamental work in security was made by Cachin in the late 90's [9] in the context of steganography. Cachin interprets the attempt of an attacker to distinguish between an innocent image and a stego-content as a hypothesis testing problem. In this document, the basic properties of a stegosystem are defined using the notions of entropy, mutual information, and relative entropy. Mittelholzer [24], inspired by the work of Cachin, proposed the first theoretical framework for analyzing the security of a watermarking scheme.

These efforts to bring a theoretical framework for security in steganography and watermarking, have been followed up by Kalker [20] who tries to clarify the concepts (robustness *vs.* security) and the classifications of watermarking attacks. This work has been deepened by Furon *et al.* [16], who have translated Kerckhoffs' principle (Alice and Bob shall only rely on some previously shared secret for privacy) from cryptography to data hiding. They used Diffie and Hellman methodology, and Shannon's cryptographic framework [29].

These attacks have been classified into categories, according to the type of information Eve has access to [12], [27]:

- Watermarked Only Attack (WOA): the attacker has access only to watermarked contents.
- Known Message Attack (KMA): the attacker has access to pairs of watermarked contents and corresponding hidden messages.
- Known Original Attack (KOA): occurs when an attacker has access to several pairs of watermarked contents and their corresponding original versions.
- Constant-Message Attack (CMA): the attacker observes several watermarked contents and only knows that the unknown hidden message is the same in all contents.

Each category of attack conducts to different security classes. For example, four classes of security are defined in [11] for WOA, namely insecurity, key-security, subspace-security and stego-security.

Barni *et al.* proposed a different approach to watermarking security, based on games with some rules concerning the public available information [6], conducting to a definition of security level similar to that proposed by Furon. Lastly, Cayre *et al.* proposed in [12] the Fisher Information Matrix to quantify security in this context.

2.2 Some reasons why unpredictability can improve security

Stego-security is clearly relevant and required in WOA setup: Eve has only access to watermarked contents and due to stego-security, it is impossible for her to decide whether a content has been processed through the embedding function or not. So in WOA setup, a stego-secure algorithm can face Eve's attacks. However, such a framework is not as useful to counteract KOA, KMA and CMA classes of attacks. In these setups, Eve tries to take benefits of its observations of watermarked contents, when she changes some initial conditions in the data hiding scheme. She desires having a sufficient understanding of the scheme and to be able to predict its behavior.

This knowledge can serve an attacker in various situations, for example when trying to counteract digital rights management (DRM), or in a man-in-the-middle attack through an hidden channel. Let us explain for example how Eve can try to achieve a man-in-the-middle attack by taking benefits of the predictable behavior of a scheme in KOA setup. We suppose that Alice and Bob communicate together through an hidden channel into some innocent master paintings. Eve has thus access to original and watermarked paintings, by using a base of knowledge and observing the communication channel. If she is able to predict the behavior of the data hiding scheme used by Alice and Bob, so when Alice send a watermarked painting P_o to Bob: Eve intercepts P_o , use the same painting P than Alice, and tries to predict how its own message should change P . The result of this prediction is sent to Bob. It is true that the chances for success for this attack are low, but these chances increase with the predictability of the data hiding scheme, thus revealing a security failure.

Let us now suppose that Eve wants to attack some DRM. She has access to several pairs of watermarks - the copyrights, which are public - and watermarked

media: we are in KMA setup. In addition, she has access to the data hiding machine, but does not have knowledge of a secret key parameter, from which the outputs of the scheme are dependent. This key thus determines the way to apply the copyright into the media. She wants to insert its own copyright in this protected media, to make it impossible to determine whether Eve is the owner or not. She does not know exactly how copyrights are applied on original media, because the DRM machine works with a secret key. However Eve can reach its goal if she is able to predict the behavior of the copyright machine: she can approximately determine what should be the watermarked media with its own copyright. As a conclusion, in various situations, unpredictable schemes should be recommended to improve security in data hiding.

2.3 Contributions in this paper

In this paper, a novel theoretical framework for data hiding security is proposed. A data hiding scheme is considered here as a machine, whose detail is public. This machine receives hidden messages and original contents from the outside world and returns stego-contents. In our point of view, security of the scheme depends on the unpredictable behavior of the machine. To give consistence to the notion of unpredictability, this machine is modeled as a dynamical system: $x^{n+1} = f(x^n)$ (where x^n denotes the n^{th} term of the sequence x). This reformulation is always possible, as it is proven in Section 3.2.

Thus, unpredictability refers to some topological or ergodic aspects of f taken from the mathematical theory of chaos, as defined by Devaney [15], Li-Yorke [22], or Adler [2] for example. This new theoretical framework for security respects Kerckhoff's principle. It is based on a topological description of data hiding, whereas most studies in this field usually have used the theory of probability [25], [17]. The goal of this research work is to give additional contribution to the variety of security evaluations which should lead to better confidence into data hiding schemes.

Compared to the information-theoretic model for steganography proposed by Cachin [9] and extended for example by Ker [21], chaotic-security appears to be a little more relevant and probably more realizable than stego-security in some particular situations, for example when chaotic sequences are used in data hiding schemes. This framework can check whether the claim of a chaotic behavior for a data hiding scheme can be verified or not. Indeed, to our best knowledge, stego-security studies often take place in WOA category and are related to Simmons' prisoners' problem [30]. In this problem, Alice and Bob are in jail and want to plan an escape by exchanging hidden messages in innocent-looking cover contents. These messages are conveyed by Eve, a warden who tries to benefit from any information leak resulting by the use of the same secret key. Quoting Cayre and Bas in [11]: "Like other works, we consider Alice and Bob use only one key. Of course, in real applications, especially in steganography, it is highly desirable to change the key at every communication between Alice and Bob." In addition, a probabilistic model of the covertext is needed and, as stated by Cachin in [9], "assuming the existence of a covertext distribution seems to

render our model somewhat unrealistic for the practical purpose of steganography". The new framework we propose does not suppose any assumption of this kind, works with simple or multiple secret keys and is not restricted to some category of attacks. Our approach is explained in detail in the following section.

3 Chaos for data hiding security

We will consider that a data hiding scheme is secure when its behavior is unpredictable. The mathematical domain that studies unpredictability is the theory of chaos, which describes the behavior of a dynamical system in topological terms. One of the most reputed description of such a chaotic behavior is due to Devaney [15]. It is recalled in the next subsection, whereas the notion of chaotic-security deduced from this definition is presented in Subsection 3.2.

3.1 Devaney's chaotic dynamical systems

Consider a metric space (\mathcal{X}, d) and a continuous function f on \mathcal{X} . Let $f^k = f \circ \dots \circ f$ denotes the k^{th} composition of a function f . Quoting Devaney in [15],

Definition 1. *f is said to be topologically transitive if, for any pair of open sets $U, V \subset \mathcal{X}$, there exists $k > 0$ such that $f^k(U) \cap V \neq \emptyset$.*

Definition 2. *An element (a point) x is a periodic element (point) for f of period $n \in \mathbb{N}^*$, if $f^n(x) = x$. The set of periodic points of f is denoted $Per(f)$.*

Definition 3. *$\{\mathcal{X}, f\}$ is said to be regular if the set of periodic points is dense in \mathcal{X} ,*

$$\forall x \in \mathcal{X}, \forall \varepsilon > 0, \exists p \in Per(f), d(x, p) \leq \varepsilon.$$

Definition 4. *f has sensitive dependence on initial conditions if there exists $\delta > 0$ such that, for any $x \in \mathcal{X}$ and any neighborhood V of x , there exists $y \in V$ and $n \geq 0$ such that $|f^n(x) - f^n(y)| > \delta$.*

δ is called the constant of sensitivity of f .

Definition 5. *A function $f : \mathcal{X} \rightarrow \mathcal{X}$ is said to be chaotic on \mathcal{X} if $\{\mathcal{X}, f\}$ is regular, topologically transitive and has sensitive dependence on initial conditions.*

When f is chaotic, then the system $\{\mathcal{X}, f\}$ is chaotic and quoting Devaney [15]: "it is unpredictable because of the sensitive dependence on initial conditions. It cannot be broken down or simplified into two subsystems which do not interact because of topological transitivity. And in the midst of this random behavior, we nevertheless have an element of regularity". Fundamentally different behaviors are consequently possible and occurs in an unpredictable way.

3.2 Chaotic-security

As stated before, we believe that an unpredictable behavior is required for a data hiding scheme to satisfy an efficient level of security. This unpredictability makes it difficult to determine whose coefficients of the cover media will be altered during the embedding of the watermark, which limits the possibilities of Eve in KOA and KMA attacks. The scheme should at least be chaotic according to Devaney: this property will improve the ability of Alice and Bob to withstand attacks. Indeed, it will be as difficult for Eve to find the hidden message after n iterations than to forecast the weather after n days without mistakes: because of chaos, this last becomes impossible to do in practice when n increases. Due to Devaney's chaos, such a "chaotic-secure" information hiding scheme will thus satisfy sensitive dependence to the initial condition, regularity and transitivity. Sensitivity to initial conditions is useful, among other, to withstand sensitivity attack [14] (it can be noticed that, in the context of the sensitivity attack, various strategies have been already employed [18]). In addition, sensitivity is helpful to achieve authentication, because the watermark's embedding will be highly dependent on any changes of the carrier image. Moreover, fragile data hiding is achieved with a large constant of sensitivity. Transitivity trends to improves robustness: for example, Eve cannot hope to remove the watermark by cropping the media. Indeed, the system will visit all the space, so the watermark will be uniformly distributed on the whole media. This property improves authentication, as this last can be achieved by studying any part of the media: theoretically speaking, authentication still remains possible in a cropped media. Transitivity trends to improve security too, as Eve cannot have a better understanding of the scheme, cannot reduce its complexity by studying only a well chosen reduced part of the watermarked content. Lastly, transitivity and regularity lead to unpredictability, which helps Alice and Bob to withstands KOA and KMA attacks. For these reasons we believe that this new point of view could enrich the field of security in data hiding.

Let us now present more rigorously the new notion of chaotic-security. To check whether an existing data hiding scheme is chaotic or not, we propose firstly to write it as an iterate process $x^{n+1} = f(x^n)$. It is possible to prove that this formulation can always be done. Let us consider a given data hiding algorithm. It is always possible to translate it as a Turing machine and this last can be written as $x^{n+1} = f(x^n)$ by the following way. Let (w, i, q) be the current configuration of the Turing machine (Fig. 1), where $w = \sharp^{-\omega} w(0) \dots w(k) \sharp^{\omega}$ is the paper tape, i is the position of the tape head, q is used for the state of the machine, and δ is its transition function. We define f by:

- $f(w(0) \dots w(k), i, q) = (w(0) \dots w(i-1)aw(i+1)w(k), i+1, q')$,
if $\delta(q, w(i)) = (q', a, \rightarrow)$,
- $f(w(0) \dots w(k), i, q) = (w(0) \dots w(i-1)aw(i+1)w(k), i-1, q')$,
if $\delta(q, w(i)) = (q', a, \leftarrow)$.

Thus the Turing machine can be written as an iterate function $x^{n+1} = f(x^n)$ on a well-defined set \mathcal{X} , with x^0 as the initial configuration of the machine. We denote by $\mathcal{T}(S)$ the iterative process of a data hiding scheme S .

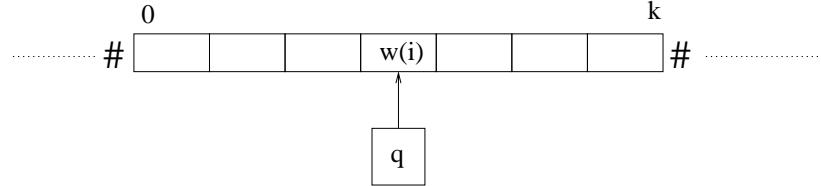


Fig. 1. Turing Machine

Let d be a relevant distance on \mathcal{X} . So the behavior of this dynamical system can be studied to know whether the data hiding scheme is unpredictable or not. This leads to the following definition.

Definition 6. *An information hiding scheme S is said to be chaotic-secure on (\mathcal{X}, d) if its iterative process $\mathcal{T}(S)$ has a chaotic behavior according to Devaney.*

Theoretically speaking, chaotic security can always be studied, as it only requires that the two following points are satisfied.

- Firstly, the data hiding scheme must be written as an iterate function on a set \mathcal{X} . We have stated that this is possible for any given scheme.
- Secondly, a metric or a topology must be defined on \mathcal{X} . This is always possible, for example by taking either the discrete or the trivial topology, even though these last are not really relevant for the aims we want to reach.

Chaotic-security is clearly impacted by the choice of the distance or topology on \mathcal{X} and this dependence must be regarded with attention. It is evident that the choice of the metric (or of the topology) must be justified, for example by establishing a strong link between the proximity of two points and the aims that data hiding attempts to reach. However, some topologies are more natural and reasonable than others, and equivalence of topologies reduces the impact of this choice. In addition, it can be remarked that stego-security supposes the same kind of hypothesis: dealing with probabilities implies the definition of a sigma-algebra. To our best knowledge, the Borel algebra is always chosen, even though this choice is neither stated, nor justified. As a topological space is needed to define Borel sets, we can claim that at least when a stego-security study is possible, so a chaotic study can be realized, with a topology inherited from the stego-security study (which justifies its choice).

In our point of view, the chaotic-security is the lowest level of security for a data hiding scheme in terms of unpredictability. This property is required, but is not sufficient: it is only the first stage of the evaluation of the unpredictable

behavior of the scheme. This study must be followed by the establishment of the list of chaotic properties that the system presents. Indeed, being unpredictable is a tricky thing to define and the number of candidates that give consistence to this notion is large. Namely topological and metric entropy, ergodicity, topological mixing, lyapunov exponent, expansivity, transitivity and strong transitivity, bifurcation theory, or chaos as defined by Li-Yorke, by Devaney or by Knudsen to name a few. As each definition illustrates a particular aspect of an unpredictable behavior and has its own interest, each notion of chaos offers a new light on the security of a data hiding scheme. Thus we consider that a given data hiding scheme will be more secure than another one if it presents a larger number of chaotic qualities and if its quantitative values are better. Indeed the properties to check is depending on the aims to reach: fragile watermarking, robustness, *etc.* This point is illustrated in the next section and will be largely deepened in a future work.

4 Chaotic-security of spread-spectrum data hiding schemes

4.1 A first proof of chaotic-security

In what follows, our framework is used to give a first chaotic-security evaluation of the well-known spread-spectrum (SS) data hiding techniques [11]. This proves that the previous framework is ready for real-world applications and establishes a concrete link between chaotic and stego-security notions.

Let $x \in \mathbb{R}^{N_v}$ be an host vector in which we want to hide a message $m \in \{0; 1\}^{N_c}$. N_c is the size of the hidden payload (in bits) and N_v the size of the stego or host vector (in samples). A key \mathcal{K} is used to initialize a PRNG (Pseudo-Random Number Generator) to obtain N_c secret carries $\{u^i\}$ taken in \mathbb{R}^{N_v} . Thus in classical SS the watermark signal w is constructed as follows:

$$w = \sum_{i=0}^{N_c-1} \gamma(-1)^{m^i} u^i \quad (1)$$

where γ is a given distortion level. The watermarked signal y is then defined by:

$$y = x + w \quad (2)$$

Let us now suppose that the components of the watermark are bounded by a finite value N : $\max(\{w_i, i \in \llbracket 1, N_v \rrbracket\}) \leq N$. This bound can be as large as needed, however a very large N seems to be contradictory with the aims of a data hiding scheme. Let us consider $\mathcal{X} = ([0, N]^{N_v})^N \times \mathbb{R}^{N_v}$ and

$$G((S, E)) = (\sigma(S); i(S) + E) \quad (3)$$

where σ is the *shift* function defined by $\sigma : (S^n)_{n \in \mathbb{N}} \in \left([0, N]^{N_v}\right)^{\mathbb{N}} \rightarrow (S^{n+1})_{n \in \mathbb{N}} \in \left([0, N]^{N_v}\right)^{\mathbb{N}}$ and the *initial function* i is the map which associates to a sequence, its first term: $i : (S^n)_{n \in \mathbb{N}} \in \left([0, N]^{N_v}\right)^{\mathbb{N}} \rightarrow S^0 \in [0; N]^{N_v}$.

Spread-spectrum data hiding techniques are thus the result of N_c iterations of the following dynamical system:

$$\begin{cases} X^0 \in \mathcal{X}, \\ X^{n+1} = G(X^n), \end{cases} \quad (4)$$

and the watermarked media is the second component of X^{N_c} .

Classical SS, *i.e.* with BPSK modulation [11], is defined by $X^0 = (S^0, E^0)$ where E^0 is the host vector x and S^0 is the sequence

$$\left((-1)^{m^0} \gamma u^0, (-1)^{m^1} \gamma u^1, \dots, (-1)^{m^{N_c-1}} \gamma u^{N_c-1}\right), \quad (5)$$

in which γ allows to achieve a given distortion, whereas in ISS (Improved Spread Spectrum [23]), S^0 is defined by

$$\left((-1)^{m^i} \alpha - \frac{\langle x, u^i \rangle}{\|u^i\|^2}\right)_{i=0, \dots, N_c-1}, \quad (6)$$

where α and λ are computed to achieve an average distortion and to minimize the error probability [11]. Lastly, in natural watermarking NW, S^0 is defined by

$$\left(-\left(1 + \eta(-1)^{m^i} \frac{\langle x, u^i \rangle}{|\langle x, u^i \rangle|}\right) \frac{\langle x, u^i \rangle}{\|u^i\|^2}\right)_{i=0, \dots, N_c-1}. \quad (7)$$

This modulation consists in a model-based projection on the different vectors u^i followed by a η -scaling along the direction of u^i . Natural watermarking has been proven stego-secure in [11].

We will prove in what follows that spread-spectrum data hiding schemes are chaotic-secure, *i.e.* that G is chaotic on (\mathcal{X}, d) , thus finding a first chaotic and stego-secure algorithm.

Let $d_\infty(A, B) = \max \{|A_i - B_i|, i = 1 \dots N_v\}$ be one of the usual metrics on \mathbb{R}^{N_v} . We define a new distance between two points $X = (S, E), Y = (\check{S}, \check{E}) \in \mathcal{X}$ by $d(X, Y) = d_\infty(E, \check{E}) + d_s(S, \check{S})$, where $d_s(S, \check{S}) = \frac{9}{N} \sum_{k=0}^{\infty} \frac{d_\infty(S^k, \check{S}^k)}{10^k}$.

The choice of d_∞ on \mathbb{R}^{N_v} is not important, because of the equivalence of norms in finite dimension: as topologies are the same, thus chaotic properties does not change by using another distance on \mathbb{R}^{N_v} . d_s has been chosen such that $d(X, Y)$ is small when the distance between the watermarked images resulting on the spread-spectrum applied on X and Y are close (for any metrics on \mathbb{R}^{N_v} , as they are all equivalent). Lastly, $\frac{9}{N}$ is just a normalization value.

We will now prove that:

Proposition 1. *G is continuous on (\mathcal{X}, d) .*

Proof. We use the sequential continuity. Let $(S_n, E_n)_{n \in \mathbb{N}}$ be a sequence of the phase space \mathcal{X} , which converges to (S, E) . We will prove that $(G(S_n, E_n))_{n \in \mathbb{N}}$ converges to $G(S, E)$. Let us recall that for all n , S_n is a strategy, thus, we consider a sequence of strategies (*i.e.* a sequence of sequences).

As $d((S_n, E_n); (S, E))$ converges to 0, each distance $d_\infty(E_n, E)$ and $d_s(S_n, S)$ converges to 0.

1. If $\frac{9}{N} \sum_{k=0}^{\infty} \frac{d_\infty(S_n^k, S^k)}{10^k} \rightarrow 0$ when $n \rightarrow \infty$, then $\frac{9}{N} \sum_{k=1}^{\infty} \frac{d_\infty(S_n^k, S^k)}{10^k} \rightarrow 0$. So $\frac{9}{N} \sum_{k=0}^{\infty} \frac{d_\infty(S_n^{k+1}, S^{k+1})}{10^{k+1}} = \frac{1}{10} d_s(\sigma(S_n); \sigma(S)) \rightarrow 0$. As a consequence, $d_s(\sigma(S_n), \sigma(S))$ converges to 0.
2. Let us prove that $d_\infty(i(S_n) + E_n; i(S) + E) \rightarrow 0$.

$$\begin{aligned} d_\infty(i(S_n) + E_n; i(S) + E) &= \max \{ |(i(S_n)_k + (E_n)_k) - (i(S)_k + E_k)|, k = 1 \dots N_v \} \\ &= \max \{ |(i(S_n)_k - i(S)_k) + ((E_n)_k - E_k)|, k = 1 \dots N_v \} \\ &\leq \max \{ |i(S_n)_k - i(S)_k|, k = 1 \dots N_v \} + d_\infty(E_n, E) \\ &= d_\infty(S_n^0, S^0) + d_\infty(E_n, E) \\ &\leq d_s(S_n, S) + d_\infty(E_n, E) \\ &= d((S_n, E_n); (S, E)) \rightarrow 0. \end{aligned}$$

Proposition 2. *Periodic points of G are dense in \mathcal{X} , so G is regular.*

Proof. Let $(S, E) \in \mathcal{X}$ and $\varepsilon > 0$. We are looking for a periodic point $(\check{S}, \check{E}) \in \mathcal{X}$ such that $d((S, E), (\check{S}, \check{E})) < \varepsilon$. Let $\check{E} = E$ and S_n denotes the sequence defined by:

$$\begin{cases} S_n^k = S^k & \forall k \leq n \\ S_n^k = (N, \dots, N) & \text{if } k > n \text{ and } k \equiv 0 \pmod{2} \\ S_n^k = (-N, \dots, -N) & \text{else.} \end{cases}$$

Then $d_s(S_n, S) = \frac{9}{N} \sum_{k=n+1}^{\infty} \frac{d_\infty(S_n^k, S^k)}{10^k} \leq \frac{9}{N} \sum_{k=n+1}^{\infty} \frac{N}{10^k} = \frac{1}{10^n} \rightarrow 0$ when $n \rightarrow \infty$. So $\exists n_0 \in \mathbb{N}$ such that $d_s(S^{n_0}, S) < \varepsilon$. The point (S^{n_0}, E) is then a periodic point of \mathcal{X} which is ε -close to the given point (S, E) .

We will now prove that,

Proposition 3. *G is transitive on \mathcal{X} .*

Proof. Let $B_A = \mathcal{B}(X_A, r_A)$ and $B_B = \mathcal{B}(X_B, r_B)$ be two open balls of \mathcal{X} , where $X_A = (S_A, E_A)$ and $X_B = (S_B, E_B)$. We are looking for $\tilde{X} = (\tilde{S}, \tilde{E}) \in B_A$ such that $\exists n_0 \in \mathbb{N}, G^{n_0}(\tilde{X}) \in B_B$.

Let $k_0 \in \mathbb{Z}$ such that $10^{-k_0} \leq r_A < 10^{-k_0+1}$ and $(\check{S}, \check{E}) = G^{k_0}(X_A)$. We define $\tilde{X} = (\tilde{S}, \tilde{E})$ as below:

- $\tilde{E} = E_A$,
- $\forall k \leq k_0, \tilde{S}^k = S_A^k$,
- $\forall k \in \llbracket 1, N_v \rrbracket, \tilde{S}^{k_0+k} = (-\check{E}^k + E_B^k) \times (0, \dots, 0, 1, 0, \dots, 0)$, i.e. the vector \tilde{S}^{k_0+k} has its components null, except its k^{th} , equals to $(-\check{E}^k + E_B^k)$,
- $\forall k \in \mathbb{N}, \tilde{S}^{k_0+N_v+k+1} = S_B^k$.

With such a definition, \tilde{X} is in B_A and satisfies $G^{k_0+N_v}(\tilde{X}) \in B_B$.

As G is regular and transitive on (\mathcal{X}, d) , we can conclude that G is sensitive to initial conditions (using the result of Banks [5]), thus proving that G is chaotic in the meaning of Devaney. As a conclusion,

Theorem 1. *Spread-spectrum data hiding techniques are chaotic-secure.*

All the variety of SS techniques are concerned by this property of chaotic-security. In the point of view presented above, the choice of NW instead of ISS only affects the initial condition of the iterations of G . Indeed, the theory of chaos gives a global approach of the unpredictable behavior of a given system, but does not explain how to choose a good initial condition. For example, the reputed logistic map $X^0 \in [0, 1], X^{n+1} = 4X^n(1 - X^n)$, has a chaotic behavior, but if we choose $X^0 = 0$, then $\forall n \in \mathbb{N}, X^n = 0$... We believe that stego-security is helpful to determine the initial values: to increase the security level of a given scheme, we thus recommend to use a chaotic-secure algorithm with stego-secure initial conditions. This discussion will be deepened in details in a future work.

4.2 Qualitative and quantitative evaluation

As stated before, the proof that a given data hiding scheme is chaotic-secure, is just the beginning of the study. The next stage is to evaluate the quality of its chaotic behavior, by using the numerous qualitative and quantitative tools offered by the theory of chaos. These tools allow to compare two given chaotic-secure schemes, by deciding which scheme is the most unpredictable and thus must be preferred. To give illustration, some tools are recalled in this section, namely strong transitivity, and the constants of expansivity and sensitivity. We will use them to give a better understanding of the unpredictability of spread-spectrum techniques.

Qualitative property: Strong transitivity

Definition 7. *A discrete dynamical system $\{\mathcal{X}, f\}$ is said to be strongly transitive if and only if, for any point $A, B \in \mathcal{X}$ and any neighborhood V of B , $n_0 \in \mathbb{N}$ and $X \in V$ can be found such that $f^n(X) = A$.*

We have the result,

Proposition 4. *$\{\mathcal{X}, G\}$ is strongly transitive.*

Proof. Let us reconsider the proof of the transitivity of (\mathcal{X}, G) : we have defined $\tilde{X} \in B_A$ such that $G^{k_0+N_v}(\tilde{X}) \in B_B$. Indeed, for this \tilde{X} , we have: $G^{k_0+N_v}(\tilde{X}) = X_B$.

Quantitative measures One of the most famous measure in the theory of chaos is the constant of sensitivity defined in Definition 4. Intuitively, a function f having a constant sensitivity equal to δ implies that there exists points arbitrarily close to any point x which *eventually* separate from x by at least δ under some iterations of f . This induces that an arbitrarily small error on an initial condition may magnified upon iterations of f . The sensitive dependence on the initial conditions is a consequence of regularity and transitivity [5]. However, the constant of sensitivity can be obtained by proving the sensitivity without Banks' theorem.

Proposition 5. *Spread-spectrum data hiding techniques $\{\mathcal{X}, G\}$ have sensitive dependence on initial conditions and its constant of sensitivity is equal to $\frac{N}{2}$.*

Proof. Let $X = (S, E) \in \mathcal{X}$, $B = \mathcal{B}(X, r)$ an open ball centered in X , and $k_0 \in \mathbb{Z}$ such that $10^{-k_0} \leq r < 10^{-k_0+1}$. We define \check{X} by:

- $\check{E} = E$,
- $\check{S}^k = S^k$, $\forall k \in \mathbb{N}$ such that $k \neq k_0 + 1$,
- if $S_1^{k_0+1} < \frac{N}{2}$, then $\check{S}_1^{k_0+1} = N$, else $\check{S}_1^{k_0+1} = 0$,
- $\forall i \in \llbracket 2, N_v \rrbracket$, $\check{S}_i^{k_0+1} = S_i^{k_0+1}$.

So $d(X, \check{X}) = D_\infty(E, \check{E}) + d_S(S, \check{S}) = 0 + \frac{9}{N} \frac{d_\infty(S^{k_0+1}, \check{S}^{k_0+1})}{10^{k_0+1}} \leq \frac{9}{N} \frac{N}{10^{k_0+1}} \leq \frac{1}{10^{k_0}} \leq r$, then $\check{X} \in B$. Let us now define $\mathcal{E} : \mathcal{X} \rightarrow \mathcal{X}$, $(S, E) \mapsto E$. So $\mathcal{E}(G^{k_0+1}(X))_0 = \mathcal{E}(G^{k_0+1}(\check{X}))_0$, because $E = \check{E}$ and $S^k = \check{S}^k, \forall k \leq k_0 + 1$. As:

- $\mathcal{E}(G^{k_0+2}(X))_0 = \mathcal{E}(G^{k_0+1}(X))_0 + S_0^{k_0+1}$,
- $\mathcal{E}(G^{k_0+2}(\check{X}))_0 = \mathcal{E}(G^{k_0+1}(\check{X}))_0 + \check{S}_0^{k_0+1}$,
- $|S_0^{k_0+1} - \check{S}_0^{k_0+1}| \geq \frac{N}{2}$.

We thus have $d(G^{k_0+2}(X), G^{k_0+2}(\check{X})) \geq d_\infty(\mathcal{E}(G^{k_0+2}(X)), \mathcal{E}(G^{k_0+2}(\check{X}))) \geq |\mathcal{E}(G^{k_0+2}(X))_0 - \mathcal{E}(G^{k_0+2}(\check{X}))_0| \geq \frac{N}{2}$.

Let us now recalled another usual quantitative measure of disorder.

Definition 8. *A function f is said to have the property of expansivity if*

$$\exists \varepsilon > 0, \forall x \neq y, \exists n \in \mathbb{N}, d(f^n(x), f^n(y)) \geq \varepsilon.$$

Then ε is the *constant of expansivity* of f : an arbitrarily small error on any initial condition is always amplified till ε .

Proposition 6. *$\{\mathcal{X}, G\}$ is not an expansive chaotic system.*

Proof. Let $\varepsilon > 0$. We define: $X = (O_{N_v}; (O_{N_v}, O_{N_v}, \dots, O_{N_v}, \dots))$ and $Y = \left(O_{N_v}; \left(\frac{\varepsilon}{2} I_{N_v}, -\frac{\varepsilon}{2} I_{N_v}, \dots, \frac{(-1)^n \varepsilon}{2} I_{N_v}, \dots\right)\right)$, where $O_{N_v} = (0, \dots, 0)$ is the null vector of size N_v and I_{N_v} is the vector of size N_v equal to $(1, 0, \dots, 0)$. Thus, for this two points, we have: $\forall n \in \mathbb{N}, d(G^n(X); G^n(Y)) \leq \varepsilon$.

4.3 Discussion

Let us give now some consequences of this qualitative and quantitative evaluation. First of all, we can regret that spread-spectrum is not expansive. This property reduces drastically the benefits that Eve can obtain of an attack in KMA or KOA setup. For example, it is impossible to have an estimation of the watermark by moving the message (or the cover) as a cursor in situation of expansivity: this cursor will be too much sensible and the changes will be too much important to be useful. On the contrary, a very large constant of expansivity ε is unsuitable: the cover media will be strongly altered whereas the watermark should be undetectable. Indeed, let us consider the same cover twice with two different watermarks. Thus $d(X, Y) < 1$ for the distance defined previously. However, due to expansivity, $\exists n \in \mathbb{N}, d(G^n(X); G^n(Y)) \geq \varepsilon$. Thus, $d_\infty(G^n(X)_1; G^n(Y)_1) \geq \varepsilon - 1$, so either $d_\infty(X_1; G^n(X)_1) \geq \frac{\varepsilon - 1}{2}$, or $d_\infty(Y_1; G^n(Y)_1) \geq \frac{\varepsilon - 1}{2}$. If ε is large, then at least one of the two watermarked media will be very different than its original cover. Due to strong transitivity, the set of watermarked media obtained when using a fixed watermark, is equal to the whole set of media. In that situation, Eve cannot reduce the set of media to studied, reducing so the interest of a Constant-Message Attack setup for Eve. The importance of the sensitivity has been explained previously.

We will now discuss various consequences of the introduction of this new framework for security. Firstly, new comparisons can be done between given data hiding schemes, as it is illustrated by the following example. In a previous work [4], we have proven that a famous tool in discrete dynamical systems, namely chaotic iterations, satisfies the Devaney's definition of chaos and we have proposed various applications of this tool in information security [31], [19], [4]. These chaotic iterations can be used to realize a data hiding scheme, as it is explained in [3]. Qualitative and quantitative chaotic tools introduced in Section 4 can thus be used to compare this algorithm to the spread-spectrum data hiding schemes. It can be proven that data hiding schemes based on chaotic iterations are chaotic secure, with the additional property of strong transitivity, as it is the case of spread-spectrum. However, chaotic iteration data hiding schemes have a larger constant of sensitivity than spread-spectrum and contrary to this last, chaotic iterations are expansive (with a constant of expansivity equal to 1). Moreover, chaotic iterations are topologically mixing, proving so that chaotic iterations appear to be more suitable than spread-spectrum to withstand attacks in KOA, KMA and CMA setup. All these claims will be proven in a future work.

5 Conclusion and future work

In this paper, a new concept of security for data hiding schemes is proposed as a complementary approach to the existing framework. This new notion of security contributes to the reinforcement of confidence into existing secure data hiding schemes. Moreover, it can replace stego-security in situations that are

not encompassed by it. In particular, this framework is more relevant to give evaluation of data hiding schemes based on chaotic maps.

In our approach, a data hiding scheme is secure if it is unpredictable. Its iterative process must satisfy the Devaney's chaos property and its level of security increases with the number of chaotic properties satisfied by it. This point has been clarified in Section 4, in which a first study of chaotic-security is proposed using some qualitative and quantitative tools taken from the mathematical theory of chaos.

We have shown in this paper that the intersection between the two sets of stego-secure and chaotic-secure data hiding algorithms is nonempty, due to spread-spectrum techniques. This establishes a first connection between the two approaches for security in data hiding. In future work, we will discuss with more attention this fact, to give a better understanding of the links between these two frameworks. The comparison between spread-spectrum and chaotic iterations outlined in Section 4.3 will be deepened. In addition, new tools taken from the theory of chaos will be introduced to enrich chaotic-security. Moreover, these tools will be compared to the Fisher Information Matrix and other information theoretic measures. The security of other existing schemes will be studied in the framework of chaos, to compare them to spread-spectrum and chaotic iterations. We will thus wonder whether chaotic iterations are stego-secure, or not. Last, but not least, the way to understand these chaotic tools in terms of data hiding aims will be deepened: this study is required to make chaotic-security framework really useful in practice.

References

1. A. Adelsbach, S. Katzenbeisser, and A.-R. Sadeghi. A computational model for watermark robustness. In Camenisch et al. [10], pages 145–160.
2. R. L. Adler, A. G. Konheim, and M. H. McAndrew. Topological entropy. *Trans. Amer. Math. Soc.*, 114:309–319, 1965.
3. J. M. Bahi and C. Guyeux. A watermarking algorithm satisfying topological chaos properties. *CoRR*, abs/0810.4713, 2008.
4. J. M. Bahi and C. Guyeux. Topological chaos and chaotic iterations, application to hash functions. In *WCCI'10: 2010 IEEE World Congress on Computational Intelligence*, 2010. Accepted paper.
5. J. Banks, J. Brooks, G. Cairns, and P. Stacey. On devaney's definition of chaos. *Amer. Math. Monthly*, 99:332–334, 1992.
6. M. Barni, F. Bartolini, and T. Furon. A general framework for robust watermarking security. *Signal Processing*, 83(10):2069–2084, 2003. Special issue on Security of Data Hiding Technologies, invited paper.
7. M. Barni, I. J. Cox, T. Kalker, and H. J. Kim, editors. *IWDW'05: 4th International Workshop on Digital Watermarking*, volume 3710 of *Lecture Notes in Computer Science*, Siena, Italy, September 15-17 2005. Springer.
8. S. Battiato, D. Catalano, G. Gallo, and R. Gennaro. Robust watermarking for images based on color manipulation. In Pfitzmann [28], pages 302–317.
9. C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192:41 – 56, 2004.

10. J. Camenisch, C. S. Collberg, N. F. Johnson, and P. Sallee, editors. *IH 2006: Information Hiding, 8th International Workshop*, volume 4437 of *Lecture Notes in Computer Science*, Alexandria, VA, USA, July 2007. Springer.
11. F. Cayre and P. Bas. Kerckhoffs-based embedding security classes for woa data hiding. *IEEE Transactions on Information Forensics and Security*, 3(1):1–15, 2008.
12. F. Cayre, C. Fontaine, and T. Furon. Watermarking security: theory and practice. *IEEE Transactions on Signal Processing*, 53(10):3976–3987, 2005.
13. P. Comesaña, L. Pérez-Freire, and F. Pérez-González. Fundamentals of data hiding security and their application to spread-spectrum analysis. In *IH'05: Information Hiding Workshop*, pages 146–160. Lectures Notes in Computer Science, Springer-Verlag, 2005.
14. P. Comesaña, L. Pérez-Freire, and F. Pérez-González. The return of the sensitivity attack. In Barni et al. [7], pages 260–274.
15. R. L. Devaney. *An Introduction to Chaotic Dynamical Systems*, 2nd Edition. Westview Pr., March 2003.
16. T. Furon. Security analysis, 2002. European Project IST-1999-10987 CERTIMARK, Deliverable D.5.5.
17. T. Furon. A survey of watermarking security. In Barni et al. [7], pages 201–215.
18. T. Furon and P. Bas. Broken arrows. *EURASIP J. Inf. Secur.*, 2008:1–13, 2008.
19. C. Guyeux and J. M. Bahi. Hash functions using chaotic iterations. *Journal of Algorithms & Computational Technology*, 2009. To appear.
20. T. Kalker. Considerations on watermarking security. pages 201–206, 2001.
21. A. D. Ker. Batch steganography and pooled steganalysis. In Camenisch et al. [10], pages 265–281.
22. T. Y. Li and J. A. Yorke. Period three implies chaos. *Amer. Math. Monthly*, 82(10):985–992, 1975.
23. H. Malvar and D. Florêncio. Improved spread spectrum: A new modulation technique for robust watermarking. *IEEE Trans. Signal Proceeding*, 53:898–905, 2003.
24. T. Mittelholzer. An information-theoretic approach to steganography and watermarking. In Pfitzmann [28], pages 1–16.
25. L. Perez-Freire, P. Comesana, J. R. Troncoso-Pastoriza, and F. Perez-Gonzalez. Watermarking security: a survey. In *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.
26. L. Pérez-Freire, F. Pérez-González, T. Furon, and P. Comesaña. Security of lattice-based data hiding against the known message attack. *IEEE Trans. on Information Forensics and Security*, 1(4):421–439, dec 2006.
27. L. Perez-Freire, F. Pérez-gonzalez, and P. Comesaña. Secret dither estimation in lattice-quantization data hiding: A set-membership approach. In E. J. Delp and P. W. Wong, editors, *Security, Steganography, and Watermarking of Multimedia Contents*, San Jose, California, USA, January 2006. SPIE.
28. A. Pfitzmann, editor. *IH'99: 3rd International Workshop on Information Hiding*, volume 1768 of *Lecture Notes in Computer Science*, Dresden, Germany, September 29 - October 1. 2000. Springer.
29. C. E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28:656–715, 1949.
30. G. J. Simmons. The prisoners' problem and the subliminal channel. In *Advances in Cryptology, Proc. CRYPTO'83*, pages 51–67, 1984.
31. Q. Wang, C. Guyeux, and J. M. Bahi. A novel pseudo-random number generator based on discrete chaotic iterations. In *INTERNET'09: First International Conference on Evolving Internet*, pages 71–76, 2009.